

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-110543

(P2003-110543A)

(43) 公開日 平成15年4月11日(2003.4.11)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード*(参考)
H 0 4 L 9/08		H 0 4 L 12/28	3 0 0 A 5 J 1 0 4
12/28	3 0 0	9/00	6 0 1 D 5 K 0 3 3

審査請求 有 請求項の数10 O L (全 8 頁)

(21) 出願番号 特願2001-298631(P2001-298631)

(22) 出願日 平成13年9月27日(2001.9.27)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 波多野 健

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

(72) 発明者 鍛冶 孝一

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5J104 AA16 EA26 NA02

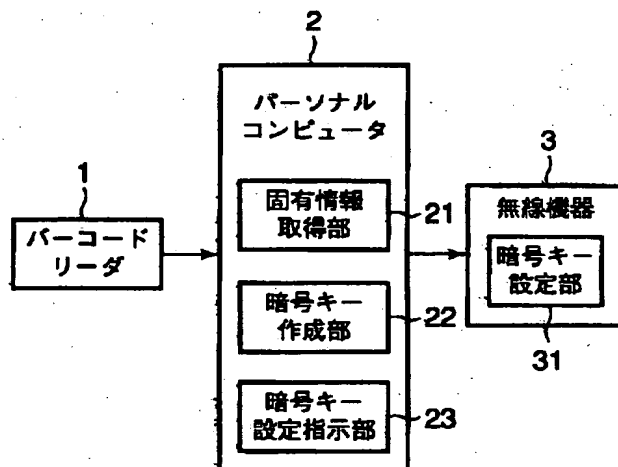
5K033 AA08 DA17 EC01

(54) 【発明の名称】 暗号キー設定システム、無線通信装置および暗号キー設定方法

## (57) 【要約】

【課題】暗号キーが初期設定のままの状態を利用して  
もセキュリティを維持することを実現する暗号キー設定  
システムを提供する。

【解決手段】無線機器3は、この暗号キー設定システム  
で処理対象とする、たとえば製造・販売元の出荷製品で  
あり、パーソナルコンピュータ2の固定情報取得部21  
は、バーコードリーダ1を用いて無線機器3に固有の情報、  
たとえば製造番号やMACアドレスなどを取得する。  
また、暗号キー作成部22は、この固定情報取得部  
21により取得された情報を利用して、無線機器3が無  
線通信時に用いる暗号キーを作成する。そして、暗号キ  
ー設定指示部23は、この暗号キー作成部22が作成し  
た暗号キーを設定させるための命令を無線機器3に向  
けて発行する。一方、この命令を受け取った無線機器3  
では、暗号キー設定部31が、この暗号キーの設定を実行  
する。



## 【特許請求の範囲】

【請求項 1】 無線通信装置が有する機器固有情報を取得する固有情報取得手段と、

前記固有情報取得手段により取得された機器固有情報を用いて前記無線通信装置が無線通信を行う際のデータ暗号キーを作成する暗号キー作成手段と、  
前記暗号キー作成手段により作成された暗号キーを前記無線通信装置に設定する設定手段とを具備することを特徴とする暗号キー設定システム。

【請求項 2】 前記固有情報取得手段は、前記無線通信装置の製造番号を取得することを特徴とする請求項 1 記載の暗号キー設定システム。

【請求項 3】 前記固有情報取得手段は、前記無線通信装置に割り当てられた MAC アドレスを取得することを特徴とする請求項 1 記載の暗号キー設定システム。

【請求項 4】 前記固有情報取得手段は、バーコードリーダにより前記機器固有情報を読み取ることを特徴とする請求項 1、2 または 3 記載の暗号キー設定システム。

【請求項 5】 前記暗号キー作成手段は、ESS-ID を作成することを特徴とする請求項 1、2、3 または 4 記載の暗号キー設定システム。

【請求項 6】 前記暗号キー作成手段は、WEP キーを作成することを特徴とする請求項 1、2、3 または 4 記載の暗号キー設定システム。

【請求項 7】 前記設定手段により前記無線通信装置に設定した暗号キーを当該システムが動作する装置に設定する第 2 の設定手段を具備することを特徴とする請求項 1、2、3、4、5 または 6 記載の暗号キー設定システム。

【請求項 8】 無線通信を行う際のデータ暗号キーの初期設定指示を入力する入力手段と、

前記入力手段により前記初期設定指示が入力されたときに、自装置が有する機器固有情報を取得する固有情報取得手段と、

前記固有情報取得手段により取得された機器固有情報を用いて暗号キーを作成する暗号キー作成手段と、  
前記暗号キー作成手段により作成された暗号キーを自装置に設定する設定手段とを具備することを特徴とする無線通信装置。

【請求項 9】 無線通信装置が有する機器固有情報を取得する固有情報取得ステップと、

前記固有情報取得ステップにより取得された機器固有情報を用いて前記無線通信装置が無線通信を行う際のデータ暗号キーを作成する暗号キー作成ステップと、  
前記暗号キー作成ステップにより作成された暗号キーを前記無線通信装置に設定する設定ステップとを具備することを特徴とする暗号キー設定方法。

【請求項 10】 無線通信を行う際のデータ暗号キーの初期設定指示を入力する入力ステップと、

前記入力ステップにより前記初期設定指示が入力された

ときに、自装置が有する機器固有情報を取得する固有情報取得ステップと、

前記固有情報取得ステップにより取得された機器固有情報を用いて暗号キーを作成する暗号キー作成ステップと、

前記暗号キー作成ステップにより作成された暗号キーを自装置に設定する暗号キー設定ステップとを具備することを特徴とする暗号キー設定方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、たとえば無線 LAN アクセスポイント等の無線通信装置に暗号キーを設定するための暗号キー設定システム、自装置の暗号キーを設定する機能を有する無線通信装置および暗号キー設定方法に係り、特に、暗号キーが初期設定のままの状態でも利用されてもセキュリティを維持することを実現する暗号キー設定システム、無線通信装置および無線通信方法に関する。

## 【0002】

【従来の技術】近年、無線 LAN (IEEE802.11b) や Bluetooth などといった、パーソナルエリアの無線通信システムが注目されている。また、この種の無線通信システムでは、無線の特性上、電波を傍受されるおそれがあることや、ネットワーク環境に誰でも接続可能となるおそれがあることから、セキュリティの維持のために、暗号キーによって接続認証を行う機能をもっている。

【0003】そこで、ユーザは、互いに無線通信を行わせたい複数の無線通信装置間で同期させて、同一の暗号キーを各々設定するなどといった作業を行っていた。

【0004】たとえば、IEEE802.11におけるセキュリティとしては、WEP (Wired Equivalent Privacy) キーと呼ばれる 40 ビットの暗号化されたコードを用いることで、同じ WEP コードを持つ無線機器以外からの接続を許可しないようにするものや、SSID (Service Set ID) と呼ばれる無線機器間でのグループ設定を行うものが知られている。

## 【0005】

【発明が解決しようとする課題】しかしながら、ユーザの中には、セキュリティ維持の意識が低い者も少なからず見受けられ、暗号キーを考慮することなく、無線通信装置を使い始めてしまうユーザも存在するのが現状である。

【0006】一方、無線通信装置の製造・販売元では、ユーザによる暗号キーの設定を想定しているため、一般的には、暗号キーを設定せずに、または、所定の暗号キーを暫定的に設定して出荷している。したがって、ユーザが出荷時の初期設定のままの状態でも無線通信装置を使用すると、無関係な相手との通信が行われてしまうといった事態が発生しうる。つまり、たとえば無線 LAN を構築するためのアクセスポイントがこのような状態で使

用されると、不正なユーザからの侵入を許すことにもなってしまう。

【0007】この発明は、このような事情を考慮してなされたものであり、暗号キーが初期設定のままの状態でも利用されてもセキュリティを維持することを實現する暗号キー設定システム、無線通信装置および無線通信方法を提供することを目的とする。

【0008】

【課題を解決するための手段】前述した目的を達成するために、この発明の暗号キー設定システムは、無線通信装置が有する機器固有情報を取得する固有情報取得手段と、前記固有情報取得手段により取得された機器固有情報を用いて前記無線通信装置が無線通信を行う際のデータ暗号キーを作成する暗号キー作成手段と、前記暗号キー作成手段により作成された暗号キーを前記無線通信装置に設定する設定手段とを具備することを特徴とする。

【0009】この暗号キー設定システムにおいては、たとえば製造・販売元からの出荷時などにおいて、製造番号やMAC(Media Access Control)アドレスなど、無線通信装置に固有の情報を取得し、その固有情報から暗号キーを作成して、それぞれの無線通信装置に設定する。

【0010】すなわち、この暗号キー設定システムでは、製品1つ1つに固有の暗号キーを割り当てるといった非常に手間がかかる、従来であれば非現実的であった作業を自動化することにより、ユーザが出荷時と同じ初期設定のままの状態でも無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを實現する。

【0011】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。

【0012】(第1実施形態)まず、この発明の第1実施形態について説明する。

【0013】図1は、この第1実施形態に係る暗号キー設定システムの全体図である。図1に示すように、この暗号キー設定システムでは、バーコードリーダ1とパーソナルコンピュータ2とが接続され、さらに、このパーソナルコンピュータ2と無線機器3とが接続される。この無線機器3は、たとえば無線LANアクセスポイントなどであり、この暗号キー設定システムで処理対象とする、たとえば製造・販売元の出荷製品である。

【0014】また、パーソナルコンピュータ2は、固有情報取得部21、暗号キー作成部22および暗号キー設定指示部23を備え、無線機器3は、暗号キー設定部31を備えている。

【0015】図2は、このパーソナルコンピュータ2の機器構成を示す図である。このパーソナルコンピュータ2は、たとえばデスクトップタイプやノートブックタイプのコンピュータであり、図2に示すように、CPU1

01、DRAM102、HDD103、表示コントローラ104、キーボードコントローラ105およびI/Oコントローラ106を有している。

【0016】CPU101は、このパーソナルコンピュータ2の動作を統合的に制御するものであり、DRAM102に格納されたユーティリティソフトウェアaを含む各種プログラムの記述にしたがって各部の動作を制御する。また、ユーティリティソフトウェアaは、このパーソナルコンピュータ2を暗号キー設定システムとして動作させるためのプログラムであり、HDD103から適宜ロードされてDRAM102に格納される。そして、図1で示した固有情報取得部21、暗号キー作成部22および暗号キー設定指示部23は、このユーティリティソフトウェアaによって實現される。

【0017】DRAM102は、このパーソナルコンピュータ2の主記憶となるメモリデバイスであり、ユーティリティソフトウェアaを含む各種プログラムや、これらのプログラムから入出力される各種データを格納する。また、HDD103は、このパーソナルコンピュータ2の外部記憶となるメモリデバイスであり、DRAM102の2次記憶として各種プログラムおよび各種データを大量に格納する。

【0018】表示コントローラ104は、このパーソナルコンピュータ2におけるユーザインタフェースのアウトプットを司るものであり、CPU101が作成した表示データをCRTやLCDに表示する。一方、キーボードコントローラ105は、このパーソナルコンピュータ2におけるユーザインタフェースのインプットを司るものであり、キーボードやマウスの操作を数値化してCPU101に引き渡す。

【0019】また、I/Oコントローラ106は、外部機器との間の有線による通信を制御するものであり、バーコードリーダ1や無線機器3とは、このI/Oコントローラ106が備えるインタフェースコネクタを介して接続される。

【0020】図3は、無線機器3の機器構成を示す図である。この無線機器3は、無線LAN(IEEE802.11b)規格に準拠した無線通信を行うものであり、図3に示すように、CPU201、EEPROM202、フラッシュメモリ203、DRAM204、無線通信部205、表示コントローラ206およびI/Oコントローラ207を有している。

【0021】IEEE802.11b方式では、ISM(Industrial Scientific Medical)バンドと呼ばれる2.4GHz帯を使用して無線通信を行ない、送受信信号の変調方式として、直接拡散方式のスペクトル拡散通信(DSSS: Direct Sequence Spread Spectrum)を用いている。さらに、2.4GHz帯(2.4000~2.4835GHz)を14のチャネル(国によっては使用チャネルが制限される)に分割して使用する。各チャネルの占有

帯域は、各チャネルの中心周波数から±11MHzの22MHzである。この通信チャネルは、無線通信を行う機器間で同一のチャネルを使用するように設定される。

【0022】CPU201は、この無線機器3の動作を統合的に制御するものであり、フラッシュメモリ203に格納された暗号キー設定プログラムcを含む各種プログラムの記述にしたがって各部の動作を制御する。また、暗号キー設定プログラムcは、EEPROM202に格納される、無線通信時の接続認証に利用される暗号キーbを設定するためのプログラムである。この暗号キー設定システムでは、たとえばIEEE802.11bで規定されたWEP (Wired Equivalent Privacy) キーやESS-ID (Extended Service Set-ID) を暗号キーbとして取り扱う。そして、図1で示した暗号キー設定部31は、この暗号キー設定プログラムcによって実現される。

【0023】EEPROM202は、暗号キーbを含む各種設定情報を格納するメモリデバイスであり、フラッシュメモリ203は、暗号キー設定プログラムcを含む各種プログラムを格納するメモリデバイスである。また、DRAM204は、CPU201の作業領域となるメモリデバイスである。

【0024】無線通信部205は、他の無線機器との間の無線による通信を制御するものであり、IEEE802.11bの無線機能を制御するベースバンドLSI、このベースバンドLSIが実行するプログラムを格納するフラッシュメモリ、アンテナおよびベースバンドLSIとアンテナとの間における高周波信号の制御を行なうRF部を具備している。

【0025】表示コントローラ206は、この無線機器3におけるユーザインタフェースのアウトプットを司るものであり、CPU201が作成した表示データをLCDに表示する。一方、I/Oコントローラ207は、この無線機器3におけるユーザインタフェースのインプットを司るものであり、各種ボタンの押下をCPU201に通知する。また、このI/Oコントローラ207は、外部機器との間の有線による通信の制御も行い、パーソナルコンピュータ2とは、このI/Oコントローラ207が備えるインタフェースコネクタを介して接続される。

【0026】次に、このような機器構成をもつこの暗号キー設定システムの動作について説明する。図4は、この暗号キー設定システムの動作手順を示すフローチャートである。

【0027】たとえば無線機器3の製造・販売元で、その出荷時に無線機器3の暗号キーbを設定する場合、まず、オペレータが、パーソナルコンピュータ2のユーティリティソフトウェアaを起動する(ステップA1)。

【0028】ユーティリティソフトウェアaが起動されると、固定情報取得部21、暗号キー作成部22および

暗号キー設定指示部23が作動するので、オペレータは、バーコード化されて受注伝票などに印刷された無線機器3の製造番号やMACアドレスなどをバーコードリーダー1で読み取る。このバーコードリーダー1で読み取られた製造番号やMACアドレスなどは、無線機器3に固有の情報として固有情報取得部21が取得する(ステップA2)。

【0029】また、固有情報取得部21は、この取得した情報を暗号キー作成部22に転送する。一方、暗号キー作成部22は、この転送された情報を利用して、無線機器3が無線通信時に用いる暗号キーを作成する(ステップA3)。この暗号キー作成部22による暗号キーの作成は、たとえば製造番号またはMACアドレスの一部または全部に所定の手順でスクランブルをかけるなど、ある規則性を持たせることができれば、つまり再現できればどのような方法であってもよい。また、たとえば桁合わせなどを行うのみで、この製造番号またはMACアドレスの一部または全部をそのまま暗号キーとしても構わない。

【0030】そして、暗号キー設定指示部23は、この暗号キー作成部22が作成した暗号キーを設定させるための命令を、I/Oコントローラ106を介して無線機器3に向けて発行する(ステップA4)。一方、この命令をI/Oコントローラ207を介して受け取った無線機器3では、暗号キー設定部31が、この暗号キーをEEPROM202に格納する(ステップA5)。

【0031】以降、オペレータは、パーソナルコンピュータ2と接続する無線機器3を交換していきながら、前述の処理を繰り返す。

【0032】このように、この実施形態の暗号キー設定システムでは、各無線機器3に固有の暗号キーを簡単に設定することを可能としており、ユーザが出荷時と同じ初期設定のままの状態で無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

【0033】(第2実施形態) 次に、この発明の第2実施形態について説明する。

【0034】図5は、この第2実施形態に係る暗号キー設定システムの全体図である。前述した第1実施形態の暗号キー設定システムとこの第2実施形態の暗号キー設定システムとの違いは、図5に示すように、無線機器3自身が、暗号キー作成部32を備える点にある。この暗号キー作成部32は、パーソナルコンピュータ2から暗号キーを設定する旨の命令が発行されたときに、たとえば自装置に割り当てられたMACアドレスをEEPROM202から読み出し、この読み出したMACアドレスを利用して、自機器が無線通信時に用いる暗号キーを作成する。

【0035】これに伴い、パーソナルコンピュータ2で

10

20

30

40

50

は、バーコード1との接続と固有情報取得部21および暗号キー作成部22とが不要となり、また、暗号キー設定指示部23は、(暗号キーの転送を伴わない)暗号キーを設定する旨の命令を無線機器3に発行する機能のみを備えればよい。

【0036】図6は、この第2実施形態の暗号キー設定システムの動作手順を示すフローチャートである。

【0037】たとえば無線機器3の製造・販売元等のオペレータは、まず、パーソナルコンピュータ2のユーティリティソフトウェアaを起動する(ステップB1)。ユーティリティソフトウェアaが起動されると、暗号キー設定指示部23が作動するので、オペレータは、この暗号キー設定指示部23に、暗号キーを設定させるための命令を、I/Oコントローラ106を介して無線機器3に向けて発行させる(ステップB2)。

【0038】一方、この命令をI/Oコントローラ207を介して受け取った無線機器3では、暗号キー作成部32が、たとえば自装置に割り当てられたMACアドレスから無線通信時に用いる暗号キーを作成する(ステップB3)。そして、暗号キー設定部31が、この暗号キー作成部32により作成された暗号キーをEEPROM202に格納する(ステップB4)。

【0039】以降、オペレータは、パーソナルコンピュータ2と接続する無線機器3を交換していきながら、前述の処理を繰り返す。

【0040】このように、この実施形態の暗号キー設定システムも、各無線機器3に固有の暗号キーを簡単に設定することを可能とし、ユーザが出荷時と同じ初期設定のままの状態無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

【0041】なお、ここでは、パーソナルコンピュータ2からの命令に応じて、暗号キー作成部32および暗号キー設定部31が作動する例を示したが、この暗号キーを設定する旨を指示するためのボタンを無線機器3に設け、このボタンの操作を無線機器3のI/Oコントローラ207が検知したときに、暗号キー作成部32および暗号キー設定部31が作動するようにしてもよい。この場合には、無線機器3単体で暗号キーの設定を行うことができ、また、オペレータは、無線機器3に設けられた所定のボタンを操作すればよいことになる。

【0042】(第3実施形態)次に、この発明の第3実施形態について説明する。

【0043】図7は、この第3実施形態に係る暗号キー設定システムの全体図である。前述した第1実施形態の暗号キー設定システムとこの第3実施形態の暗号キー設定システムとの違いは、図7に示すように、パーソナルコンピュータ2側にも、暗号キー設定部24を設けた点にある。この暗号キー設定部24は、暗号キー設定指示部23から無線機器3に向けて暗号キーを設定する旨の

命令が発行されたときに、その暗号キーをパーソナルコンピュータ2にも設定する。

【0044】この第3実施形態の暗号キー設定システムでは、パーソナルコンピュータ2も処理対象、つまり、たとえば製造・販売元の出荷製品とし、かつ、このパーソナルコンピュータ2と無線機器3とがセットで出荷されて互いに無線通信を行うことを想定している。そして、このように、パーソナルコンピュータ2と無線機器3とが同期をとって同一の暗号キーを設定しなければならない場合のために、この第3実施形態の暗号キー設定システムは、これらを自動的に実行する仕組みを提供する。

【0045】図8は、この第3実施形態の暗号キー設定システムの動作手順を示すフローチャートである。

【0046】たとえば無線機器3の製造・販売元等のオペレータは、まず、パーソナルコンピュータ2のユーティリティソフトウェアaを起動する(ステップC1)。ユーティリティソフトウェアaが起動されると、固定情報取得部21、暗号キー作成部22、暗号キー設定指示部23および暗号キー設定部24が作動するので、オペレータは、バーコード化されて受注伝票などに印刷された無線機器3の製造番号やMACアドレスなどをバーコードリーダ1で読み取る。このバーコードリーダ1で読み取られた製造番号やMACアドレスなどは、無線機器3に固有の情報として固有情報取得部21が取得する(ステップC2)。

【0047】また、固有情報取得部21は、この取得した情報を暗号キー作成部22に転送する。一方、暗号キー作成部22は、この転送された情報を利用して、無線機器3が無線通信時に用いる暗号キーを作成する(ステップC3)。そして、暗号キー設定部24は、この暗号キー作成部22が作成した暗号キーを自装置のパーソナルコンピュータ2に設定する(ステップC4)。

【0048】さらに、暗号キー設定指示部23は、この暗号キー作成部22が作成した暗号キーを設定させるための命令を、I/Oコントローラ106を介して無線機器3に向けて発行する(ステップC5)。一方、この命令をI/Oコントローラ207を介して受け取った無線機器3では、暗号キー設定部31が、この暗号キーをEEPROM202に格納する(ステップC6)。

【0049】このように、この実施形態の暗号キー設定システムでは、パーソナルコンピュータ2と無線機器3との各セットごとに、固有の暗号キーを同期させながら簡単に設定することを実現する。

【0050】なお、前述した実施形態では、IEEE802.11を例に説明したが、これに限定されず、本願発明は、たとえばIEEE802.11aにも適用可能である。

【0051】つまり、本願発明は、前記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、前記

実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。たとえば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

#### 【0052】

【発明の効果】以上、詳述したように、この発明によれば、たとえば製造・販売元からの出荷時などにおいて、製造番号やMAC(Media Access Control)アドレスなど、無線通信装置に固有の情報を取得し、その固有情報から暗号キーを作成して、それぞれの無線通信装置に設定するため、ユーザが出荷時と同じ初期設定のままの状態無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

#### 【図面の簡単な説明】

【図1】この発明の第1実施形態に係る暗号キー設定システムの全体図。

【図2】同第1実施形態のパーソナルコンピュータの機器構成を示す図。

【図3】同第1実施形態の無線機器の機器構成を示す図。

【図4】同第1実施形態の暗号キー設定システムの動作手順を示すフローチャート。

【図5】同第2実施形態に係る暗号キー設定システムの全体図。

【図6】同第2実施形態の暗号キー設定システムの動作手順を示すフローチャート。

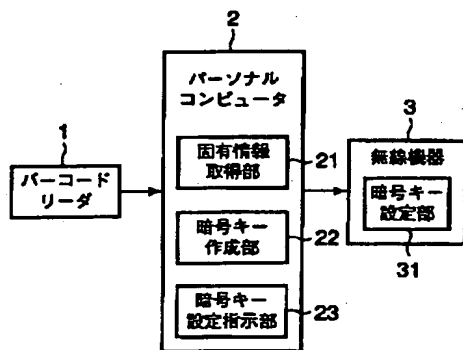
【図7】同第3実施形態に係る暗号キー設定システムの全体図。

【図8】同第3実施形態の暗号キー設定システムの動作手順を示すフローチャート。

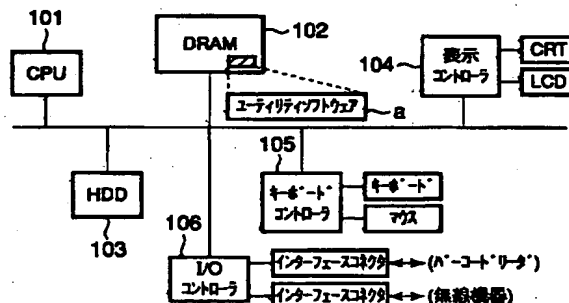
#### 【符号の説明】

- 1…バーコードリーダ
- 2…パーソナルコンピュータ
- 3…無線機器
- 21…固有情報取得部
- 22…暗号キー作成部
- 23…暗号キー設定指示部
- 24…(パーソナルコンピュータ側)暗号キー設定部
- 31…(無線機器側)暗号キー設定部
- 32…暗号キー作成部
- 101…CPU
- 102…DRAM
- 103…HDD
- 104…表示コントローラ
- 105…キーボードコントローラ
- 106…I/Oコントローラ
- 201…CPU
- 202…EEPROM
- 203…フラッシュメモリ
- 204…DRAM
- 205…無線通信部
- 206…表示コントローラ
- 207…I/Oコントローラ
- a…ユーティリティソフトウェア
- b…暗号キー
- c…暗号キー設定プログラム

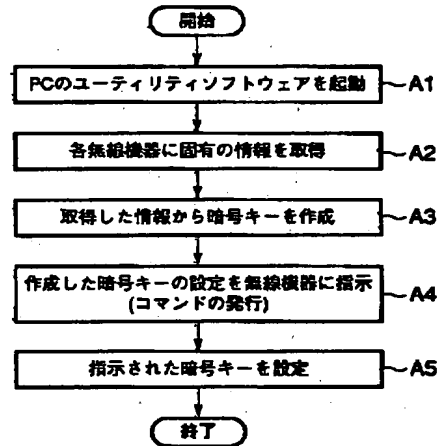
【図1】



【図2】



【図 4】

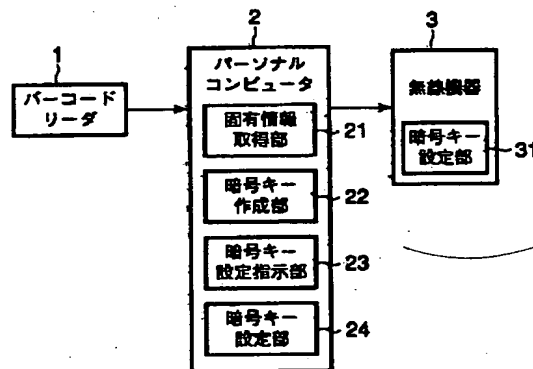


```

graph LR
    PC[パーソナルコンピュータ] --> W[無線機器]
    subgraph PC_Box [ ]
        direction TB
        PC_Label[パーソナルコンピュータ]
        CKSI[暗号キー設定指示部]
    end
    subgraph W_Box [ ]
        direction TB
        W_Label[無線機器]
        CKC[暗号キー作成部]
        CKS[暗号キー設定部]
    end
    CKSI --> W_Box
    style PC_Label fill:none,stroke:none
    style W_Label fill:none,stroke:none

```

【図 7】



【図8】

